Sicherheit und Verschlüsselung

Der Element Chat Client wird dazu auffordern ein Schlüssel Backup anzulegen. Dabei werden die Keys der Ende-zu-Ende Verschlüsselung (end-to-end encryption oder E2EE) mit einem Master-Schlüssel verschlüsselt und auf dem Matrix Server abgelegt (ähnlich einem Passwortmanager wie bspw. Keepass). Das Schlüsselbackup kann je nach Vorliebe mit einer eigenen Passphrase oder einem generierten Schlüssel verschlüsselt werden, diese beiden Optionen schlägt Element bei der Einrichtung vor, sie sind äquivalent. Ohne diese Schlüssel ist ein Entschlüsseln von verschlüsselten Nachrichten nicht mehr möglich. Auch Administratoren können hier nicht mehr helfen wenn die Schlüssel verloren werden. Es handelt sich um eine starke Verschlüsselung, das ist also so gewünscht. Matrix erlaubt für fast alle Chats und Konstellationen E2EE zu aktivieren. Auch in Chat Räumen mit mehr als 2 Teilnehmern, und auch wenn mehr als ein Matrix Server an einem Chat Raum beteiligt ist (Siehe Föderation) Damit der Austausch von Schlüsseln über mehrere Geräte/Clients hinweg zuverlässig funktioniert muss die Schlüsselsicherung aktiv sein und alle Sitzungen verifiziert werden. Alte nicht mehr genutzte und/oder nicht verifizierte Sitzungen sollten in den Einstellungen unter Sicherheit entfernt werden.

Revision #1
Created 2024-05-07 10:36:40 UTC by Philipp Offensand
Updated 2024-05-07 10:43:07 UTC by Philipp Offensand